Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Previously presented) A method for detecting spam in a messaging system comprising:

generating a white list of confirmed message senders, each of said confirmed message senders being authorized to send messages as evidenced by prior receipt of a response to a confirmation message;

distributing the white list among a plurality of spam filters in the messaging system;

using the white list at a given one of the plurality of spam filters to determine if a sender of a received message has been previously confirmed; and

forwarding the received message to a recipient without separately confirming the sender if it is determined that the sender has been previously confirmed.

2. (Previously presented) The method of claim 1 wherein the messaging system is an email system.

3. (Previously presented) The method of claim 1 wherein distributing the white list includes distributing the white list to at least two spam filters.

4. (Previously presented) The method of claim 1 wherein if the sender has not been previously confirmed, the method further includes:

sending a confirmation to the sender;

verifying a response from the sender; and

if the response is verified, adding the sender to the white list at the given spam filter and

sharing information associated with the added sender with other spam filters in the messaging system.

5. (Previously presented) The method of claim 1 wherein distributing includes publishing the white list at a central location.

6. (Previously presented) The method of claim 1 further comprising maintaining the white list at a central location, wherein using the white list includes checking the white list maintained at the central location.

7. (Previously presented) The method of claim 1 wherein if the sender has not been previously confirmed, the method further comprising:

sending a confirmation to sender;

verifying a response from the sender; and

if the response is verified, adding the sender to the white list maintained at a central location that is distributed among the plurality of spam filters.

8. (Previously presented) A method for identifying a spam message comprising:

receiving a message at a spam filter in a network that includes a plurality of spam filters, each spam filter having an associated list of confirmed senders;

identifying a sender of the message;

determining if the sender has been previously confirmed as a confirmed sender including:

determining, using a locally stored list of confirmed senders, if the sender is included in a list of confirmed senders associated with any other spam filter in the network; and

if so, forwarding the received message to a recipient without separately confirming the sender in each spam filter.

9. (Original) The method of claim 8 wherein the message is an email message.

10. (Previously presented) The method of claim 8 further comprising sharing the

locally stored list of confirmed senders with another spam filter.

11. (Previously presented) The method of claim 8, wherein if it is determined that the sender has not been previously confirmed, the method further comprising:

sending a confirmation to the sender;

verifying a response from the sender; and

if the response is acceptable, adding the sender to the locally stored list of confirmed senders and sharing information with at least one other spam filter in the network, the information including information indicating that the sender has been confirmed.

12. (Previously presented) The method of claim 11 wherein sharing information with at least one other spam filters includes publishing the locally stored list of confirmed senders at a central location that can be accessed by other spam filters.

13. (Previously presented) The method of claim 8 further comprising:

maintaining the locally stored list of confirmed senders at a central location; and

determining if the sender has been previously confirmed including checking other locally stored lists of confirmed senders associated with other spam filters at the central location.

14. (Previously presented) The method of claim 8, wherein if the sender has not been previously confirmed, the method further comprising:

sending a confirmation to the sender;

verifying a response;

if the response is acceptable, adding the sender to the locally stored list; and

distributing the locally stored list among the plurality of spam filters.

15. (Previously presented) A method for detecting a spammer in a network that includes a plurality of spam filters, the method comprising:

collecting information relating to a sender from a plurality of the spam filters;

determining a trend in the collected information; and

identifying a spammer based on the trend.

16. (Original) The method of claim 15 wherein collecting information includes collecting information relating to a number of messages sent by a sender to unrelated email addresses.

17. (Original) The method of claim 15 wherein determining trends includes correlating the messages received by an individual spam filter relating to a same sender.

18. (Previously presented) The method of claim 15 wherein identifying includes determining that a sender is a spammer if a number of messages sent to unrelated email addresses exceeds a predetermined threshold.

19. (Original) The method of claim 18 wherein the threshold is time dependent.

20. (Previously presented) A method for detecting spam in a messaging system comprising:

generating a list of confirmed message senders and maintaining the list at a data center;

receiving a message at a spam filter in a network that includes a plurality of spam filters;

verifying with the data center by the spam filter that a sender of the message is a confirmed message sender, and

if it is determined that the sender is a confirmed message sender, forwarding the received message to a recipient without separately confirming the sender.

21. (Original) The method of claim 20 wherein the message is an email message.

22. (Previously presented) The method of claim 20 further comprising sharing the list with at least two spam filters in the network.

23. (Previously presented) The method of claim 20 wherein if it is determined that the sender is not a confirmed message sender, the method further comprising:

sending, from the data center, a confirmation to the sender;

verifying a response received at the data center from the sender; and

if the response is acceptable, adding to the list of confirmed message senders a name associated with the sender; and

sharing information including the name with other spam filters in the network.

24-27. (Canceled)

28. (Previously presented) A method for detecting a spammer in a network that includes a plurality of spam filters, the method comprising:

collecting, using a data center, information relating to a sender from a plurality of the spam filters;

determining a trend in the collected information; and

identifying the sender as a spammer based on the trend including adding the sender to a list of confirmed spammers maintained by the data center.

29. (Previously presented) The method of claim 28 wherein collecting information includes collecting information relating to a number of messages sent by the sender to unrelated email addresses.

30. (Original) The method of claim 28 wherein determining trends includes correlating messages received by an individual spam filter relating to a same sender.

31. (Previously presented) The method of claim 28 wherein identifying the sender as a spammer includes determining that the sender is a spammer if a number of messages sent to unrelated email addresses exceeds a predetermined threshold.

32. (Original) The method of claim 31 wherein the threshold is time dependent.

33. (Previously presented) A method for filtering spam in a messaging system comprising:

confirming that a message sender can receive one or more messages;

distributing information indicating that the message sender can receive one or more

messages among a plurality of spam filters in the messaging system;

using said distributed information at a given one of the plurality of spam filters to determine if a message should be sent to an intended recipient without separately determining whether the message sender can receive one or more messages.

34. (Original) The method of claim 33 wherein the message is an email message.

35. (Original) The method of claim 33 further comprising confirming at a first spam filter in the system that a sender of a message can receive messages.

36. (Original) The method of claim 35 further comprising receiving the message at a second spam filter.

37. (Previously presented) The method of claim 35 further comprising distributing information developed by the first spam filter to one or more other spam filters in the messaging system.

38. (Previously presented) The method of claim 37 further comprising distributing the information to a data center, and thereafter allowing access by each of the spam filters in the messaging system to the information.

39. (Previously presented) The method of claim 33 wherein the information is maintained in a list that includes one or more confirmed message senders.

40. (Previously presented) The method of claim 39 wherein the list is distributed among a plurality of the spam filters in the messaging system.

41. (Previously presented) The method of claim 39 wherein the list is maintained by a data center accessible by the spam filters in the messaging system.

42. (Previously presented) The method of claim 41 further comprising distributing the list with a plurality of spam filters in the messaging system.

43. (Previously presented) The method of claim 42 further comprising maintaining a copy of the list at one or more of the spam filters in the messaging system.

44. (Previously presented) The method of claim 39 further comprising:

associating a passcode with one or more of the confirmed senders in the list; and

verifying a message received from a sender in the list including verifying the passcode specified by the sender.

45. (Previously presented) The method of claim 44 further comprising prompting a sender in the list to enter a passcode upon an occurrence of an predefined event.

46. (Previously presented) The method of claim 45 further comprising detecting that an email address associated with the sender has been compromised, and

prompting the sender to enter the passcode thereafter.

47. (Previously presented) The method of claim 39 further comprising:

receiving a pass code from the confirmed message sender; and

verifying the pass code is included in the message prior to forwarding the message from the confirmed message sender to the intended recipient.

48. (Original) The method of claim 47 further comprising automatically adding the passcode associated with the sender at a time for transmission of a message from the sender in the messaging system.

49. (Previously presented) The method of claim 48 further comprising providing a plug-in module for automatically adding the passcode, the plug-in module adapted to add the passcode prior to transmission to the messaging system.

50. (Previously presented) The method of claim 33 further comprising:

correlating sender-recipient data at a spam filter in the messaging system and determining data related to how fast a list of recipients grows for a given sender;

determining a list of unacceptable senders using the sender-recipient data and the determined data; and

distributing the list of unacceptable senders with other spam filters in the messaging system.

51. (Original) The method of claim 50 further comprising maintaining a list of recipients for each sender of messages processed by a given spam filter.

52. (Original) The method of claim 51 further comprising maintaining the list of recipients for each sender at a data center.

53-55. (Canceled)

56. (Previously presented) A method for minimizing spam in a messaging system, the messaging system including a plurality of spam filters, the method comprising:

receiving a request from one of the spam filters in the messaging system to verify if a sender of a message is a confirmed sender, the confirmed sender being a sender having a verified capability to receive messages;

evaluating a list of confirmed senders;

if the sender is not included in the list of confirmed senders, confirming the sender including providing a notification to the sender;

upon receipt of a confirmation from the sender in response to the notification, distributing the sender's status to other spam filters in the messaging system including adding the sender to the list; and

notifying the one spam filter indicating whether the sender's status is confirmed.

57. (Original) The method of claim 56 wherein the step of confirming the sender is performed by a spam filter.

58. (Original) The method of claim 56 wherein the step of confirming the sender is performed by the requesting spam filter.